# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP05/050729

International filing date: 18 February 2005 (18.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: FR
Number: 0402006
Filing date: 27 February 2004 (27.02.2004)

Date of receipt at the International Bureau: 02 June 2005 (02.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/EP2005/050729

R E P U B L I Q U E  F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION

## CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 14 MARS 2005

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er dépôt

INPI FEV 2004
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
INPI PARIS 34 SP
0402006

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

# BREVET D'INVENTION
## CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*03

## REQUÊTE EN DÉLIVRANCE
page 1/2

**BR1**

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 @ W / 210502

Réservé à l'INPI

REMISE DES PIÈCES
DATE
LIEU
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 27 FEV. 2004

**1** NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BALLOT
*Conseils en Propriété Industrielle*
122, rue Edouard Vaillant
92593 LEVALLOIS PERRET CEDEX
Tél. 01.49.64.61.00 - Fax 01.49.64.61.20

**Vos références pour ce dossier**
*(facultatif)* 017180 JPB/SM - GEM1568

**Confirmation d'un dépôt par télécopie** ☐ N° attribué par l'INPI à la télécopie

| **2** NATURE DE LA DEMANDE | Cochez l'une des 4 cases suivantes |
|---|---|
| Demande de brevet | ☒ |
| Demande de certificat d'utilité | ☐ |
| Demande divisionnaire | ☐ |
| *Demande de brevet initiale* | N° Date |
| *ou demande de certificat d'utilité initiale* | N° Date |
| Transformation d'une demande de brevet européen *Demande de brevet initiale* | ☐ N° Date |

**3** TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE, SUPPORT D'AUTHENTIFICATION, ET DISPOSITIF PERFECTIONNES POUR LA SECURISATION D'UN ACCES A UN EQUIPEMENT.

**4** DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

| **5** DEMANDEUR (Cochez l'une des 2 cases) | | ☒ **Personne morale** ☐ **Personne physique** |
|---|---|---|
| Nom ou dénomination sociale | | GEMPLUS |
| Prénoms | | |
| Forme juridique | | Société Anonyme |
| N° SIREN | | 3 4 9 7 1 1 2 0 0 |
| Code APE-NAF | | 3 2 1 B |
| Domicile ou siège | Rue | Avenue du Pic de Bertagne - Parc d'activités de Gemenos |
| | Code postal et ville | 1 3 4 2 0 GEMENOS |
| | Pays | FRANCE |
| Nationalité | | FRANCAISE |
| N° de téléphone *(facultatif)* | | N° de télécopie *(facultatif)* |
| Adresse électronique *(facultatif)* | | |

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION
## CERTIFICAT D'UTILITÉ

## REQUÊTE EN DÉLIVRANCE
page 2/2

**BR2**

Réservé à l'INPI

REMISE DES PIÈCES
DATE 27 FEV 2004
LIEU 75 INPI PARIS 34 SP
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0402006

DB 540 W / 210502

| | | |
|---|---|---|
| **6 MANDATAIRE** *(s'il y a lieu)* | | |
| Nom | | BENTZ |
| Prénom | | Jean-Paul |
| Cabinet ou Société | | CABINET BALLOT |
| N °de pouvoir permanent et/ou de lien contractuel | | |
| Adresse | Rue | 122, rue Edouard Vaillant |
| | Code postal et ville | 9 2 5 9 3 LEVALLOIS-PERRET CEDEX |
| | Pays | |
| N° de téléphone *(facultatif)* | | 01 49 64 61 00 |
| N° de télécopie *(facultatif)* | | 01 49 64 61 20 |
| Adresse électronique *(facultatif)* | | |
| **7 INVENTEUR (S)** | | **Les inventeurs sont nécessairement des personnes physiques** |
| Les demandeurs et les inventeurs sont les mêmes personnes | | ☐ Oui<br>☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)** |
| **8 RAPPORT DE RECHERCHE** | | **Uniquement pour une demande de brevet (y compris division et transformation)** |
| Établissement immédiat ou établissement différé | | ☒<br>☐ |
| Paiement échelonné de la redevance *(en deux versements)* | | **Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt**<br>☐ Oui<br>☐ Non |
| **9 RÉDUCTION DU TAUX DES REDEVANCES** | | **Uniquement pour les personnes physiques**<br>☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)*<br>☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : **AG** |
| **10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS** | | ☐ Cochez la case si la description contient une liste de séquences |
| Le support électronique de données est joint | | ☐ |
| La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe | | ☐ |
| **Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes** | | |

**11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE**
**(Nom et qualité du signataire)**
Levallois-Perret, le 27 février 2004

BENTZ Jean-Paul - CPI N° 99-0308

**VISA DE LA PRÉFECTURE OU DE L'INPI**

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

# PROCEDE, SUPPORT D'AUTHENTIFICATION, ET DISPOSITIF PERFECTIONNES POUR LA SECURISATION D'UN ACCES A UN EQUIPEMENT.

L'invention concerne, de façon générale, les techniques biométriques d'authentification visant à contrôler l'accès à des informations sensibles.

Plus précisément, l'invention concerne, selon un premier de ses aspects, un procédé de sécurisation d'un accès à un équipement, ce procédé comprenant au moins : une opération d'attribution consistant à fournir une donnée de référence à un support d'authentification; une opération d'acquisition consistant à obtenir, à chaque requête d'accès formulée par un demandeur d'accès à l'équipement, une signature biométrique de ce demandeur d'accès; et une étape de vérification consistant à vérifier, en utilisant la donnée de référence, l'authenticité de la signature biométrique obtenue du demandeur d'accès.

L'authentification de personnes par signature biométrique, telle par exemple qu'une empreinte digitale ou l'image de l'iris d'un œil, présente intrinsèquement une sélectivité très élevée, mais pose des problèmes spécifiques que ne pose pas l'authentification au moyen d'un code numérique personnel saisi par la personne sollicitant un accès à un équipement protéger.

En effet, dans le cas typique où l'équipement protégé comprend un ordinateur, l'authentification par code est facilement mise en œuvre en cachant le code numérique authentique fractionné dans la mémoire de l'ordinateur, en

le recomposant à chaque requête d'accès, et en comparant à l'identique le code authentique recomposé au code proposé par un demandeur d'accès.

Or, l'authentification par signature biométrique ne peut pas être mise en œuvre de la même façon dans la mesure où seules, dans ce dernier cas, peuvent être repérées des ressemblances ou des dissemblances entre une signature biométrique authentique et une signature biométrique proposée par un demandeur d'accès.

Cette singularité de l'authentification par signature biométrique oblige en pratique à mémoriser les signatures biométriques authentiques en clair sur le disque dur de l'ordinateur, de sorte qu'un pirate parvenant à accéder une seule fois à ce disque peut en retirer l'information qui lui permettra d'y accéder facilement autant de fois qu'il le souhaite par la suite en déconnectant le capteur biométrique et en injectant les données directement dans la machine cible.

L'invention a principalement pour but de proposer une solution à ce problème.

A cette fin, le procédé de l'invention, par ailleurs conforme à la définition générique qu'en donne le préambule ci-dessus, est essentiellement caractérisé en ce qu'il comporte une étape préalable de cryptage au cours de laquelle est élaborée une version cryptée d'au moins une signature biométrique authentique appartenant à au moins une personne autorisée à accéder à l'équipement, en ce que l'étape de vérification comprend une opération de décryptage mise en œuvre dans le support d'authentification

et consistant à décrypter, au moyen d'une clef secrète, la version cryptée d'une signature biométrique authentique fournie à ce support d'authentification en tant que donnée de référence lors de la requête d'accès, et en ce que l'étape de vérification comprend une opération de comparaison mise en œuvre en comparant secrètement la signature biométrique obtenue du demandeur d'accès lors de la requête d'accès à la signature biométrique authentique issue du décryptage.

Un support d'authentification pour la mise en œuvre de ce procédé prend par exemple la forme d'une carte électronique comportant au moins un module de décryptage utilisant une clef secrète, ce support pouvant en outre comporter un module de comparaison ainsi, éventuellement, qu'un module de cryptage.

L'invention concerne également un dispositif de sécurisation d'un accès à un équipement, comprenant : un support d'authentification auquel est fournie une donnée de référence; un capteur obtenant, à chaque requête d'accès formulée par un demandeur d'accès à l'équipement, une signature biométrique de ce demandeur d'accès; et des moyens de contrôle inclus dans le support d'authentification et autorisant sélectivement le demandeur d'accès à accéder à l'équipement en fonction du résultat d'une vérification de l'authenticité de la signature biométrique du demandeur d'accès au moyen de la donnée de référence, ce dispositif étant caractérisé en ce que les moyens de contrôle comprennent un module de décryptage et un module de comparaison, en ce que la donnée de référence fournie au support d'authentification est constituée par une version cryptée d'une signature biométrique authentique

supposée attribuée au demandeur d'accès, en ce que le module de décryptage utilise une clef secrète au moyen de laquelle il reconstitue secrètement, à chaque requête d'accès, la signature biométrique authentique à partir de sa version cryptée, et en ce que le module de comparaison compare secrètement la signature biométrique obtenue du demandeur d'accès à la signature biométrique authentique reconstituée, et fournit un résultat de comparaison constituant le résultat de la vérification.

Outre le support d'authentification, par exemple constituée par une carte, amovible ou non, dotée d'une mémoire non lisible de l'extérieur et dans laquelle est stockée la clef secrète, le dispositif de l'invention peut aussi comprendre un ou plusieurs ordinateurs constituant une partie au moins de l'équipement dont l'accès est sécurisé.

Dans ce cas, l'ordinateur ou l'un d'entre eux peut contenir en mémoire une pluralité de codes d'identification personnels attribués à une pluralité correspondante de personnes autorisées à accéder à l'équipement et associés à une pluralité correspondante de signatures biométriques authentiques cryptées de ces personnes autorisées, cet ordinateur pouvant alors délivrer au support d'identification, lors d'une requête d'accès, la signature biométrique authentique cryptée correspondant au code d'identification fourni par le demandeur d'accès.

Un même support d'authentification peut ainsi offrir à plusieurs personnes un accès sécurisé à l'ordinateur.

Le dispositif de l'invention peut inclure un module de cryptage propre à délivrer, en réponse à une commande de

cryptage, une version cryptée d'une signature biométrique authentique fournie en clair par le capteur.

Dans le cas où la clef secrète est une clef privée à laquelle correspond une clef publique, le module de cryptage peut avantageusement être inclus dans l'ordinateur et utiliser la clef publique du support d'authentification.

D'autres caractéristiques et avantages de l'invention ressortiront clairement de la description qui en est faite ci-après, à titre indicatif et nullement limitatif, en référence aux dessins annexés, dans lesquels :

- la figure 1 est un schéma représentant un premier mode de réalisation possible de l'invention; et

- la figure 2 est un schéma représentant un second mode de réalisation possible de l'invention.

Sur ces figures, l'équipement EQP dont l'accès est sécurisé est représenté comme incluant un ordinateur ORDI, et cet ordinateur est lui-même schématiquement représenté comme relié à un clavier CLAV, à un capteur CAPT, et à un support d'authentification CRD dont il peut partiellement contrôler le fonctionnement par une commande CMD, l'homme du métier étant en mesure de mettre en œuvre tous les moyens concrets connus, et notamment les lecteurs de cartes, pour établir les liaisons et interactions fonctionnelles représentées.

Comme annoncé précédemment, l'invention permet de sécuriser l'accès à un équipement EQP au moyen d'une authentification biométrique des personnes sollicitant l'accès à cet équipement.

Pour ce faire, l'invention utilise, de façon connue en soi, un support d'authentification CRD prenant de préférence la forme d'une carte à puce électronique, dotée d'une mémoire non lisible de l'extérieur.

A chaque requête d'accès formulée par un demandeur d'accès à l'équipement EPQ, une signature biométrique SGN du demandeur d'accès, par exemple son empreinte digitale, est détectée par le capteur CAPT et transmise au support d'authentification CRD.

Ce support d'authentification CRD vérifie alors, grâce à des moyens de contrôle CTRL dont il est doté et en utilisant une donnée de référence chiffrée stockée sur EQP ou ORDI et qui lui est fournie par EQP ou ORDI, l'authenticité de la signature biométrique SGN obtenue du demandeur d'accès, et délivre un résultat de comparaison RESULT qui déclenche ou non une autorisation d'accès à l'équipement EPQ.

Selon l'invention, la donnée de référence utilisée à chaque requête d'accès par le support d'authentification CRD est constituée par une version cryptée, telle par exemple que CRYPT_SGN02, d'une signature biométrique authentique, telle par exemple que SGN02, appartenant une personne autorisée à accéder à l'équipement.

Le procédé de l'invention comporte donc une étape préalable d'enregistrement des personnes autorisées à accéder à l'équipement EQP, au cours de laquelle est élaborée chacune des versions cryptées CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03

des signatures biométriques authentiques SGN01, SGN02, SGN03 de ces différentes personnes.

Dans le mode de réalisation de la figure 1, ce cryptage préalable est effectué dans la carte CRD, à réception d'un signal de commande CMD approprié, par un module de cryptage ENCRYPT utilisant une clef secrète K délivrée par un générateur de clef GEN_K interne à la carte CRD, ce cryptage étant réalisé sur les signatures biométriques authentiques SGN01, SGN02, SGN03 reçues du capteur CAPT et appartenant aux personnes physiquement identifiées comme étant autorisées à accéder à cet équipement.

Les versions cryptées CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03 des différentes signatures biométriques authentiques SGN01, SGN02, SGN03 sont ensuite transférées par la carte CRD, à réception d'un signal de commande CMD approprié, vers le disque dur de l'ordinateur ORDI où elles sont stockées.

Le système de cryptage utilisé est alors par exemple conforme à la norme de cryptage avancée connue de l'homme de métier sous son acronyme anglais AES (pour "Advanced Encryption Standard").

Les moyens de contrôle CTRL prévus dans la carte CRD comprennent un module de décryptage DECRYPT et un module de comparaison COMPAR.

Ainsi, pour procéder à l'authentification d'une signature biométrique SGN soumise par un demandeur d'accès, la carte CRD opère en deux temps.

Tout d'abord, le module de décryptage DECRYPT de cette carte décrypte, au moyen de la clef secrète K interne à la carte CRD, la version cryptée CRYPT_SGN02 de la signature biométrique authentique SGN02 qui est supposée être celle du demandeur d'accès, et que l'ordinateur ORDI fournit à la carte CRD en tant que donnée de référence lors de la requête d'accès.

Puis, le module de comparaison COMPAR de la carte CRD compare secrètement la signature biométrique SGN, obtenue du demandeur d'accès par l'intermédiaire du capteur CAPT lors de la requête d'accès, à la signature biométrique authentique SGN02 reconstituée par le module de décryptage à partir de sa version cryptée CRYPT_SGN02.

Enfin, le module de comparaison COMPAR fournit à l'ordinateur ORDI un résultat de comparaison RESULT, qui constitue le résultat de la vérification effectuée, et qui contient pour seule information l'indication du caractère authentique ou non de la signature biométrique SGN obtenue du demandeur d'accès.

Dans le mode de réalisation illustré à la figure 2, le générateur de clef GEN_K interne à la carte CRD fournit d'une part, en tant que clef secrète interne à cette carte, une clef privée K0, et d'autre part une clef publique K1 correspondant à cette clef privée K0 et qui peut être fournie au monde extérieur, notamment à l'ordinateur ORDI.

Dans ce mode de réalisation, les versions cryptées CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03 sont obtenues en cryptant, au moyen de la clef publique K1, les différentes signatures biométriques authentiques SGN01, SGN02, SGN03,

et ces signatures biométriques authentiques SGN01, SGN02, SGN03 sont reconstruites dans la carte CRD à partir de leurs versions cryptées CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03 au moyen d'un décryptage utilisant la clef privée K0.

Dans ces conditions, comme illustré sur la figure 2, la clef publique K1 peut être stockée dans la mémoire de masse de l'ordinateur ORDI et le module de cryptage ENCRYPT_K1 peut lui-même être prévu dans cet ordinateur, la caractéristique importante étant, comme dans le premier mode de réalisation, que les signatures biométriques authentiques SGN01, SGN02, SGN03 ne soient pas en permanence mémorisées en clair dans l'ordinateur ORDI.

Contrairement à la technique traditionnelle, dans laquelle le support d'authentification CRD contient la donnée de référence constituée par une signature biométrique en clair, l'invention prévoit que ce support ne contienne qu'une clef secrète, c'est-à-dire une information dépersonnalisée.

Dans ces conditions, l'invention ouvre la possibilité qu'un même support d'authentification CRD offre à plusieurs personnes un accès sécurisé à l'ordinateur ORDI.

La seule contrainte est que la signature biométrique de chaque demandeur d'accès puisse effectivement être comparée à une signature biométrique authentique supposée a priori attribuée à ce demandeur.

Si le nombre de personnes autorisées à accéder à l'équipement EQP est faible, il est imaginable qu'à chaque

requête d'accès l'ordinateur ORDI fournisse à la carte CRD les versions cryptées CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03 des signatures biométriques authentiques SGN01, SGN02, SGN03 de toutes les personnes autorisées à accéder à l'équipement, et que l'accès soit autorisé dès lors que l'une des signatures authentiques décryptées correspond à la signature SGN obtenue du demandeur d'accès.

Si en revanche le nombre de personnes autorisées à accéder à l'équipement EQP est relativement élevé, il peut être utile de prévoir que chaque demandeur d'accès s'identifie a priori par un code personnel tel que PIN1, PIN2, PIN3, ce code n'ayant cependant pas besoin d'être lui-même confidentiel puisqu'il ne sert qu'à sélectionner la version cryptée de signature biométrique invoquée a priori par le demandeur d'accès lors de sa requête d'accès, et non à faire droit à cette requête.

Concrètement, chaque personne autorisée à accéder à l'équipement EQP peut être identifiée, lors de l'étape préalable d'enregistrement, par un tel code personnel PIN1, PIN2, PIN3, et le code personnel de chaque personne peut être mémorisé dans l'ordinateur ORDI de manière à être mis en correspondance avec la signature biométrique authentique cryptée de cette personne.

Lors d'une requête d'accès, le demandeur d'accès peut ainsi s'identifier en composant son code personnel sur le clavier CLAV, l'ordinateur ORDI délivrant au support d'identification CRD la signature biométrique authentique cryptée, par exemple CRYPT_SGN02, correspondant au code d'identification fourni par le demandeur d'accès, par exemple PIN2.

# REVENDICATIONS

1. Procédé de sécurisation d'un accès à un équipement (EQP), ce procédé comprenant au moins : une opération d'attribution consistant à fournir une donnée de référence (CRYPT_SGN02) à un support d'authentification (CRD); une opération d'acquisition consistant à obtenir, à chaque requête d'accès formulée par un demandeur d'accès à l'équipement, une signature biométrique (SGN) de ce demandeur d'accès; et une étape de vérification consistant à vérifier, en utilisant la donnée de référence (CRYPT_SGN02), l'authenticité de la signature biométrique (SGN) obtenue du demandeur d'accès, caractérisé en ce qu'il comporte une étape préalable de cryptage au cours de laquelle est élaborée une version cryptée (CRYPT_SGN02) d'au moins une signature biométrique authentique (SGN02) appartenant à au moins une personne autorisée à accéder à l'équipement, en ce que l'étape de vérification comprend une opération de décryptage mise en œuvre dans le support d'authentification (CRD) et consistant à décrypter, au moyen d'une clef secrète (K, K0), la version cryptée (CRYPT_SGN02) d'une signature biométrique authentique (SGN02) fournie à ce support d'authentification (CRD) en tant que donnée de référence lors de la requête d'accès, et en ce que l'étape de vérification comprend une opération de comparaison mise en œuvre en comparant secrètement la signature biométrique (SGN) obtenue du demandeur d'accès lors de la requête d'accès à la signature biométrique authentique (SGN02) issue du décryptage.

2. Support d'authentification pour la mise en œuvre du procédé suivant la revendication 1, caractérisé en ce qu'il prend la forme d'une carte électronique comportant au moins

un module de décryptage (DECRYPT) utilisant une clef secrète (K, K0).

3. Support d'authentification suivant la revendication 2, caractérisé en ce qu'il comporte en outre un module de comparaison (COMPAR).

4. Support d'authentification suivant la revendication 2 ou 3, caractérisé en ce qu'il comporte en outre un module de cryptage (ENCRYPT).

5. Dispositif de sécurisation d'un accès à un équipement, ce dispositif comprenant : un support d'authentification (CRD) auquel est fournie une donnée de référence (CRYPT_SGN02); un capteur (CAPT) obtenant, à chaque requête d'accès formulée par un demandeur d'accès à l'équipement, une signature biométrique (SGN) de ce demandeur d'accès; et des moyens de contrôle (CTRL) inclus dans le support d'authentification (CRD) et autorisant sélectivement le demandeur d'accès à accéder à l'équipement (EQP) en fonction du résultat d'une vérification de l'authenticité de la signature biométrique du demandeur d'accès au moyen de la donnée de référence (CRYPT_SGN02), caractérisé en ce que les moyens de contrôle (CTRL) comprennent un module de décryptage (DECRYPT) et un module de comparaison (COMPAR), en ce que la donnée de référence (CRYPT_SGN02) fournie au support d'authentification (CRD) est constituée par une version cryptée d'une signature biométrique authentique (SGN02) supposée attribuée au demandeur d'accès, en ce que le module de décryptage (DECRYPT) utilise une clef secrète (K, K0) au moyen de laquelle il reconstitue secrètement, à chaque requête d'accès, la signature biométrique authentique (SGN02) à partir de sa version cryptée

(CRYPT_SGN02), et en ce que le module de comparaison (COMPAR) compare secrètement la signature biométrique (SGN) obtenue du demandeur d'accès à la signature biométrique authentique (SGN02) reconstituée, et fournit un résultat de comparaison (RESULT) constituant le résultat de la vérification.

6. Dispositif de sécurisation suivant la revendication 5, caractérisé en ce que le support d'authentification (CRD) est une carte, amovible ou non-amovible, dotée d'une mémoire non lisible de l'extérieur et dans laquelle est stockée la clef secrète (K, K0).

7. Dispositif de sécurisation suivant l'une quelconque des revendications 5 et 6, caractérisé en ce qu'il comprend au moins un ordinateur (ORDI) constituant une partie au moins de l'équipement (EQP) dont l'accès est sécurisé.

8. Dispositif de sécurisation suivant la revendication 7, caractérisé en ce que l'ordinateur (ORDI) contient en mémoire une pluralité de codes d'identification personnels (PIN1, PIN2, PIN3) attribués à une pluralité correspondante de personnes autorisées à accéder à l'équipement et associés à une pluralité correspondante de signatures biométriques authentiques cryptées (CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03) de ces personnes autorisées, et en ce que l'ordinateur (ORDI) délivre au support d'identification (CRD), lors d'une requête d'accès, la signature biométrique authentique cryptée (CRYPT_SGN02) correspondant au code d'identification (PIN2) fourni par le demandeur d'accès, ce dont il résulte qu'un même support d'authentification (CRD) offre à plusieurs personnes un accès sécurisé à l'ordinateur (ORDI).

9. Dispositif de sécurisation suivant l'une quelconque des revendications 5 à 8, caractérisé en ce qu'il comporte un module de cryptage (ENCRYPT, ENCRYPT_K1) propre à délivrer, en réponse à une commande de cryptage, une version cryptée d'une signature biométrique authentique fournie en clair par le capteur (CAPT).

10. Dispositif de sécurisation suivant la revendication 9, caractérisé en ce que la clef secrète (K0) est une clef privée à laquelle correspond une clef publique (K1), et en ce que le module de cryptage (ENCRYPT_K1) est inclus dans l'ordinateur (ORDI) et utilise la clef publique (K1).

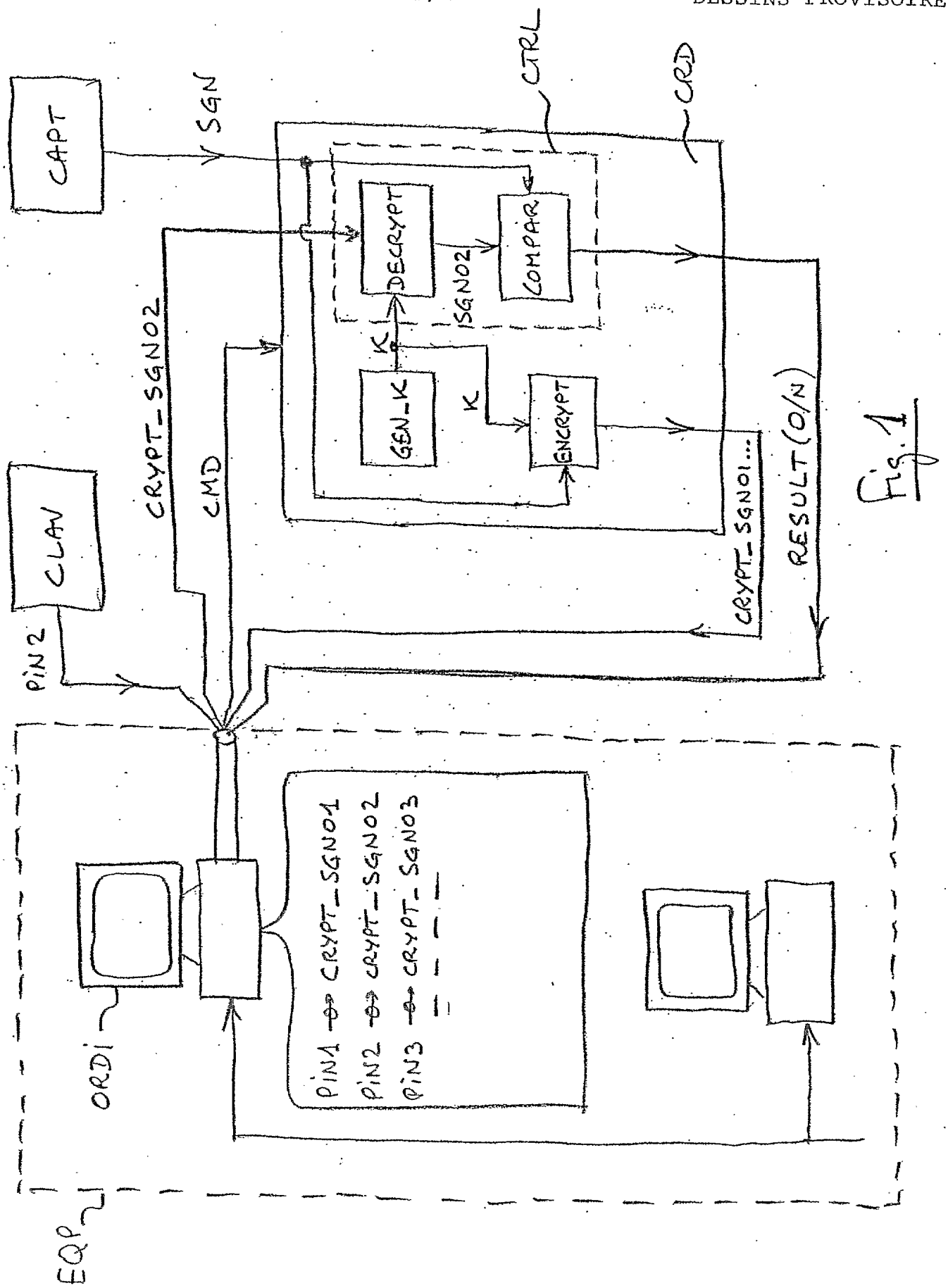
CAPT
SGN
CTRL
CRD
DECRYPT
COMPAR
ISGNO2
K
GEN_K
K
ENCRYPT
CRYPT_SGNO2
CMD
CRYPT_SGNO1...
RESULT (O/N)
CLAV
PIN2
PIN1 → CRYPT_SGNO1
PIN2 → CRYPT_SGNO2
PIN3 → CRYPT_SGNO3
ORDI
EQP

Fig. 1

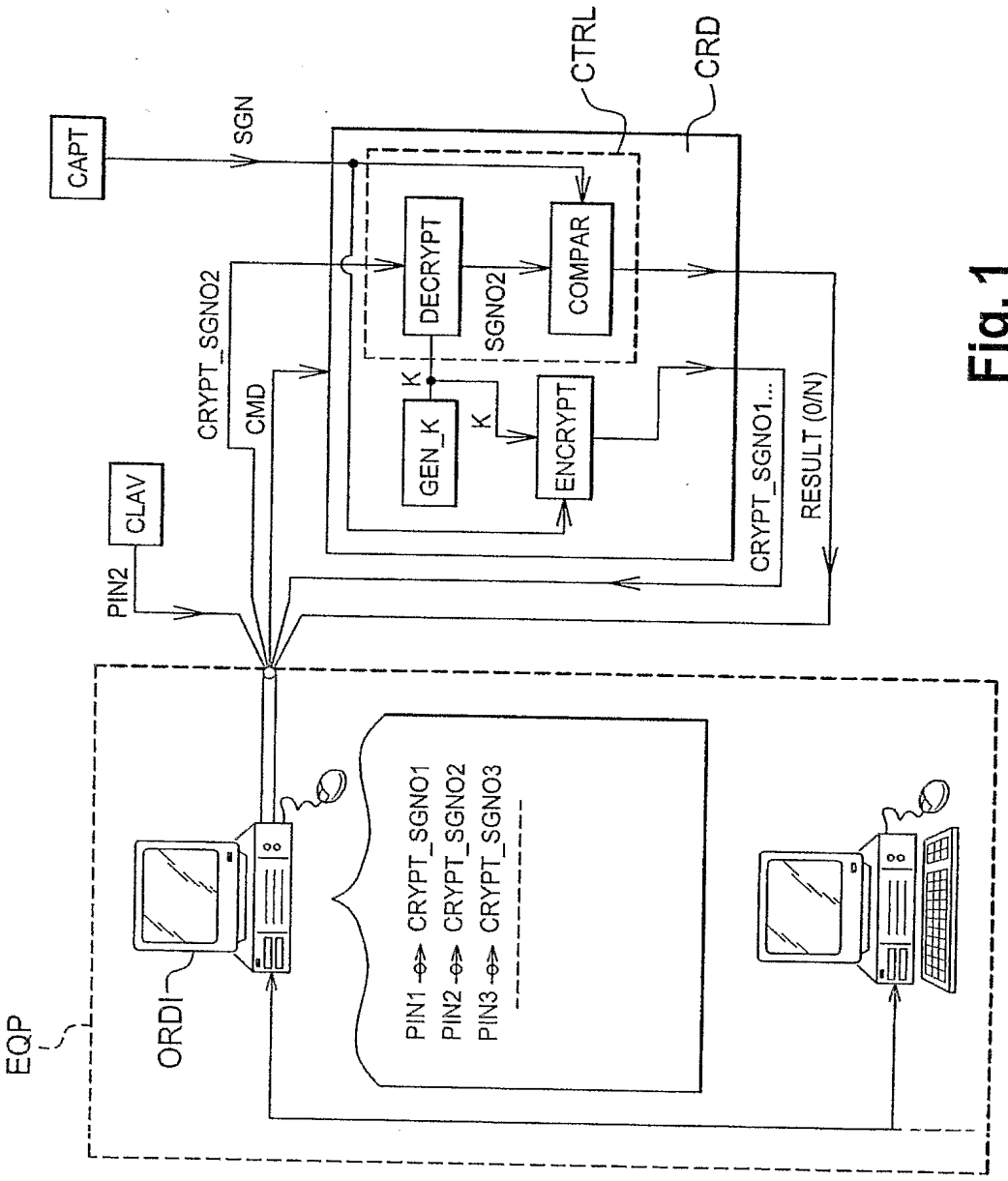
CAPT
SGN
CTRL
CRD
DECRYPT
COMPAR
SGNO2
CRYPT_SGNO2
CMD
K
K
GEN_K
ENCRYPT
CRYPT_SGNO1...
RESULT (0/N)
CLAV
PIN2
EQP
ORDI
PIN1 CRYPT_SGNO1
PIN2 CRYPT_SGNO2
PIN3 CRYPT_SGNO3

Fig. 1

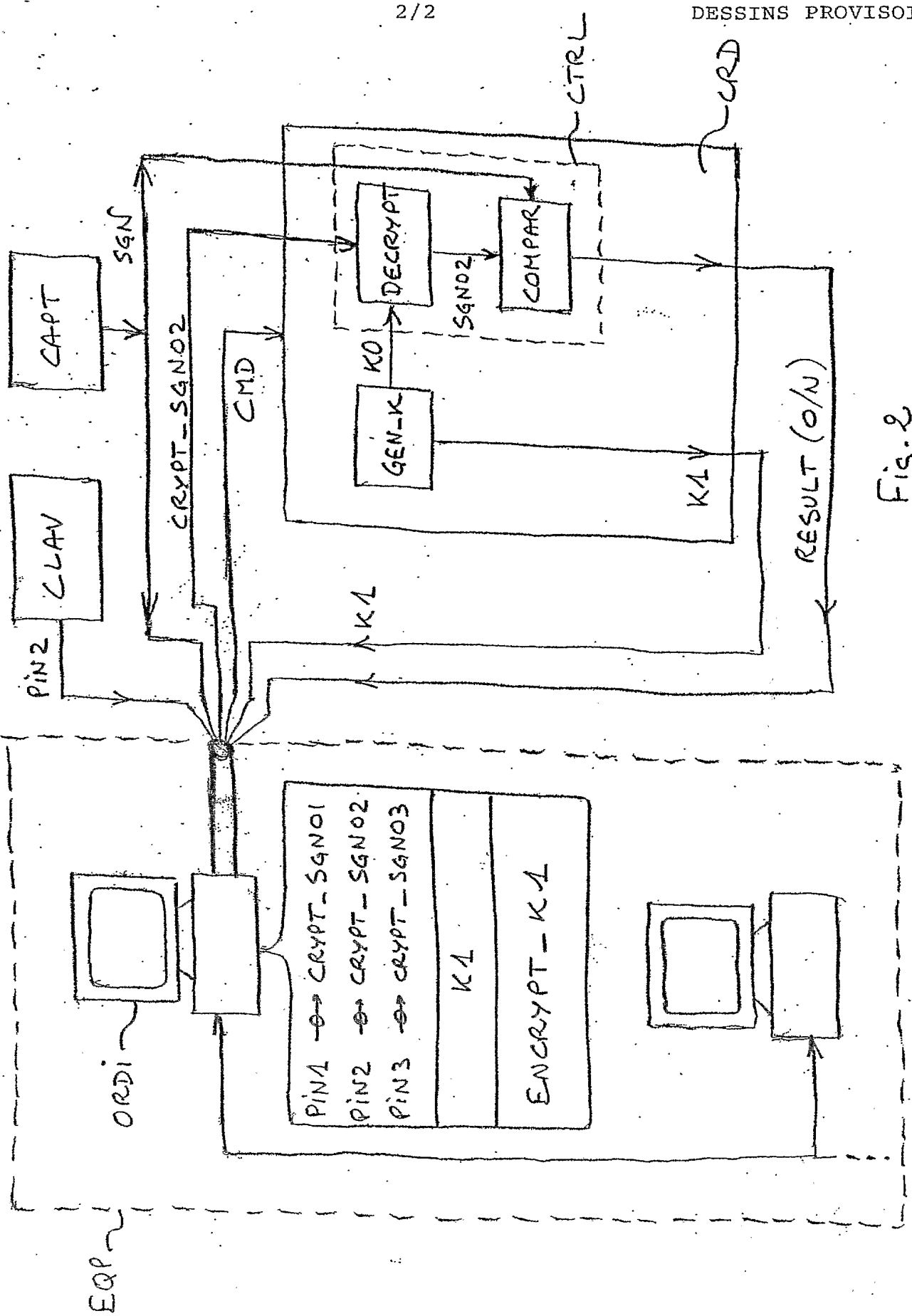
CTRL
CRD
SGN
CAPT
DECRYPT
COMPAR
SGNO2
CRYPT_SGNO2
CMD
KO
GEN-K
K1
RESULT (O/N)
CLAV
PIN2
K1
PIN1 → CRYPT_SGNO1
PIN2 → CRYPT_SGNO2
PIN3 → CRYPT_SGNO3
K1
ENCRYPT_K1
ORDI
EQP

Fig. 2

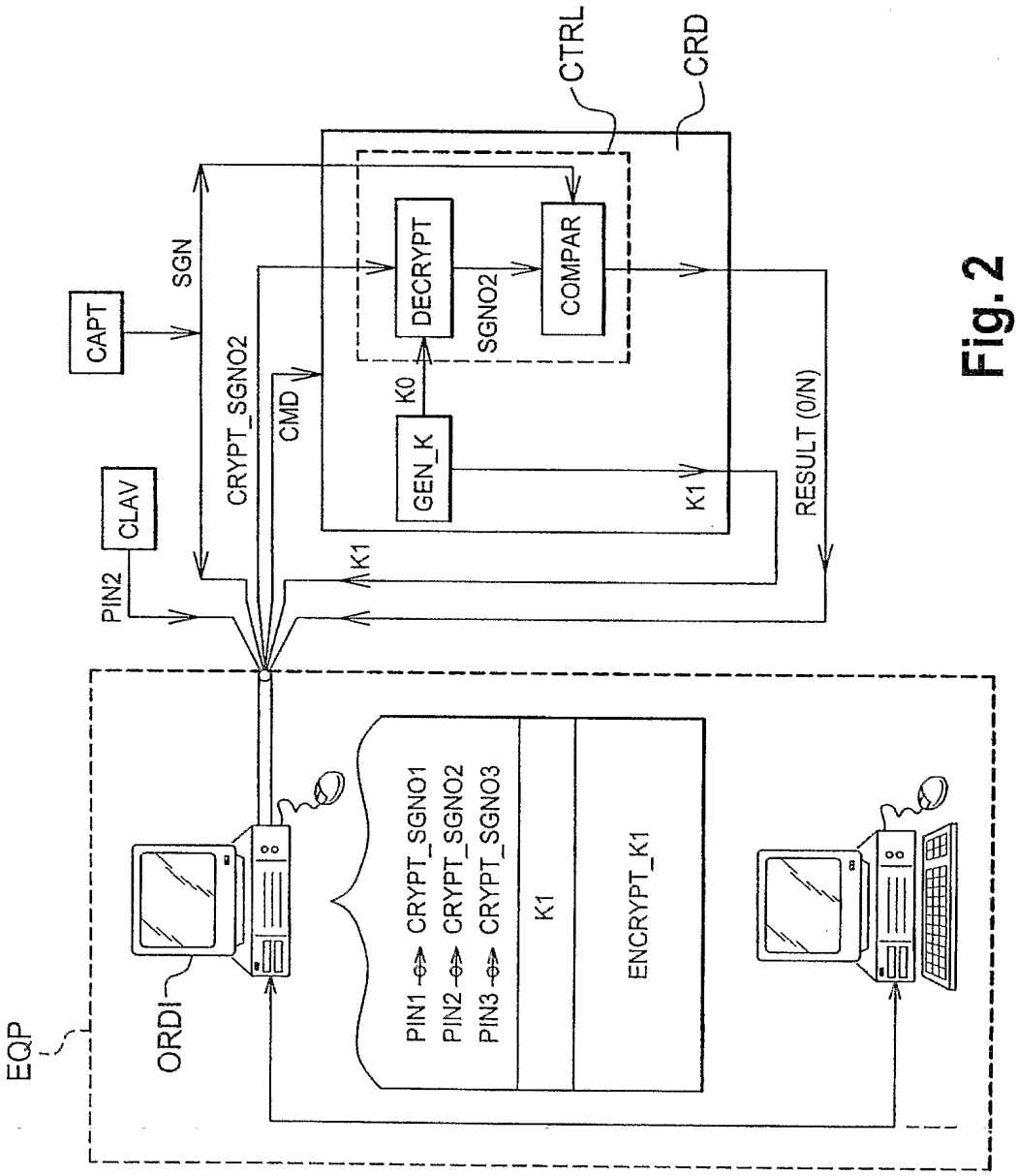
EQP
ORDI
PIN1 → CRYPT_SGNO1
PIN2 → CRYPT_SGNO2
PIN3 → CRYPT_SGNO3
K1
ENCRYPT_K1
PIN2
CLAV
CAPT
SGN
CRYPT_SGNO2
CMD
K1
CTRL
CRD
DECRYPT
COMPAR
SGNO2
K0
GEN_K
K1
RESULT (0/N)

Fig. 2

reçue le 25/03/04

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION
## CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*03

DÉPARTEMENT DES BREVETS
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

## DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

INV

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 270601

| | |
|---|---|
| **Vos références pour ce dossier** *(facultatif)* | 017180 JPB/SM - GEM1568 |
| **N° D'ENREGISTREMENT NATIONAL** | 0402006 |

**TITRE DE L'INVENTION** (200 caractères ou espaces maximum)

PROCEDE, SUPPORT D'AUTHENTIFICATION , ET DISPOSITIF PERFECTIONNES POUR LA SECURISATION D'UN ACCES A UN EQUIPEMENT.

**LE(S) DEMANDEUR(S) :**

GEMPLUS
Avenue du Pic de Bertagne
Parc d'activités de Gemenos
13420 GEMENOS
FRANCE

**DESIGNE(NT) EN TANT QU'INVENTEUR(S) :**

| | | |
|---|---|---|
| 1 Nom | | NACCACHE |
| Prénoms | | David |
| Adresse | Rue | 52, rue Letort |
| | Code postal et ville | 7 5 0 1 8 PARIS |
| Société d'appartenance *(facultatif)* | | |
| 2 Nom | | |
| Prénoms | | |
| Adresse | Rue | |
| | Code postal et ville | |
| Société d'appartenance *(facultatif)* | | |
| 3 Nom | | |
| Prénoms | | |
| Adresse | Rue | |
| | Code postal et ville | |
| Société d'appartenance *(facultatif)* | | |

**S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.**

**DATE ET SIGNATURE(S)**
**DU (DES) DEMANDEUR(S)**
**OU DU MANDATAIRE**
**(Nom et qualité du signataire)**

Levallois-Perret, le 27 février 2004
BENTZ Jean-Paul
Mandataire N° 99-0308
Cabinet BALLOT